HISCOX

Wenn Minuten entscheiden:
Cyber-Bedrohungen, Angriffszenarien & Forensik-Einblicke

Ihre Referenten: Kurzvorstellung

Lukas Reike-Kunze

Lukas Reike-Kunze,
Teammanger @HiSolutions

Martina Korch

Martina Korch, Claims Underwriter
Commercial Lines @Hiscox

Die heutigen Themen

AGENDA

- Trends aus dem Incident Response
- Schadenfälle aus der Praxis
- Best Practices

HISCOX

HISOLUTIONS

HISCOX

IT und Incident Response im Wandel

6 Trends im Incident Response

HISCOX

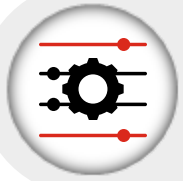
Trend 1
Ransomware verändert sich

Trend 2
Fragmentierung der Täter
und kurzlebige Marken

Trend 3
Von Einzel- zu Kumulschaden
durch gemeinsame Dienste

Trend 4
Geografische Verschiebungen

Trend 5
Staatsnahe Akteure – leise,
langfristig, strategisch



Trend 6
Governance prägt die
Einsatzarbeit

Trend 1 –
Ransomware verändert sich

- Generell: Ransomware großes Thema, aber eher rückläufig
- Bessere Backups und Cloud-Migration reduzieren Wirkung reiner Verschlüsselung
- Erpressung über Datenveröffentlichung nimmt zu → Verschlüsselung ist nicht mehr zwingend

Kosten verlagern sich zu …

Leak-Lösegeldern, IR-Aufwände, Ausfall-, Vertrags- und Meldefolgen

Trend 2 –
Fragmentierung der Täter und kurzlebige Marken

- Große „Marken“ werden gestört; es entstehen viele kleine, temporäre Crews und Rebrands
- Strafverfolgungsdruck, einfacher Namenswechsel, niedrige Eintrittsbarrieren
- Ökonomie bleibt stabil: RaaS-Anbieter, Zugangshandel, Akteure, Leak-Seiten
- Gruppennamen sind weniger aussagekräftig
- Für die Bewältigung zählen Taktikmuster, Tempo, Erpressungsstil

Trend 3 –
Von Einzel- zu Kumulschaden durchgemeinsame Dienste

- Cloud-Dienste und Managed Services Provider mit Remote Monitoring and Management sind ein Hebel: ein Vorfall, viele Betroffene
- Konsolidierung auf wenige Plattformen und starke Abhängigkeiten
- Lieferkettenfehler vervielfachen Impact und Kommunikationslast

IR-AUSWIRKUNG

- Ein Ausfall beim gemeinsamen Dienst kann hunderte Unternehmen gleichzeitig treffen
- Multi-Party-Response wird zur Standardlage: parallele Koordination mit Provider, Kunden, Versicherern, Behörden, etc.

Trend 4 –
Geografische Verschiebungen

- Europa bleibt Ziel, steht aber unter stärkerem Ermittlungs- und Compliance-Druck
- Einige Kampagnen suchen Märkte mit geringerer Sichtbarkeit – vermehrt in Asien beobachtet
- Treiber: Zahlungsbereitschaft, mediale Sichtbarkeit, regulatorische Risiken, Partnernetzwerke, etc.

Wir sehen keinen Rückzug aus Europa, aber eine teilweise Verschiebung

Trend 5 –
Staatsnahe Akteure – leise, langfristig, strategisch

- Wieder häufiger APT (Advanced Persistent Threat)
- Teilweise Geldbeschaffung zur Selbstfinanzierung, aber Hauptziel bleibt Informationsgewinnung
- Längere Verweildauern, selektive Datenabflüsse, geringe Lautstärke
- Geopolitik, wirtschaftliche Interessen, potenziellen Erstschlag vorbereiten

IR-AUSWIRKUNG

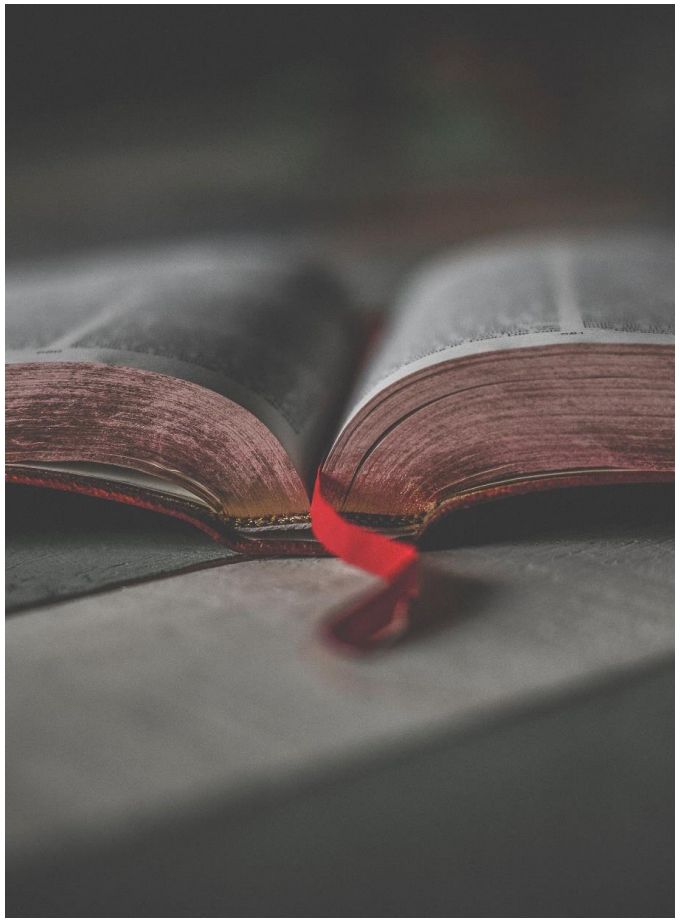
- Mehr Zeit in Lageerkundung, Diskretion in den Maßnahmen, engere Behördenzusammenarbeit

Trend 6 –
Governance prägt die Einsatzarbeit

- Melderegeln (DSGVO, NIS2, sektorale Aufsicht), Kunden- und Versicherungsanforderungen bestimmen Takt und Dokumentation der Prävention sowie Ereignisbewältigung (aber nicht bei KMU)
- Starke Professionalisierung der Technik, aber Unsicherheiten in den Abläufen
- Erhöhte Abhängig von der Technik, aber fehlende Rückfallebenen und Notfallmaßnahmen

IR-AUSWIRKUNG

- Erhöhte Bürokratie und Verwaltungsaufwand
- Lukrativere Angriffsopfer außerhalb der regulatorischen Anforderungen



Was heißt das konkret für uns im Incident Response?

HISCOX

SCHWERPUNKTVERSCHIEBUNG

- Von Ransomware zu mehr APT (Advanced Persistent Threat)
- Von Wildfang zu gezielter Auswahl
- Von System wiederherstellen zu Übersicht über große Umgebungen bekommen
- Von Einzelvorfall zu Surge-Szenarien
- Von Einzelschäden zu Multi-Party-Response
- Von Malware-Fokus zu Vertrauens- und Beziehungsmanagement (Provider, Kunden, Versicherung, Behörden, Medien, etc.)

Technik bleibt wichtig – dominiert aber nicht mehr allein den Einsatz
Angreifer suchen verstärkt einfach anzugreifende Ziele mit schlechter Resilienz aus


Weitere Fragmentierung und Professionalisierung
Leak-/Erpressungs-ökonomie wächst
Staatsnahe Präsenz in zivilen Umgebungen bleibt hoch

Ausblick

HISCOX

HISOLUTIONS

HISCOX

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com

HISCOX

Insights aus der Schaden-abteilung

Definitionen aus dem Bedingungswerk (CyberClear 01/2026)

Der Versicherungsfall

Der Versicherer gewährt den Versicherten im Rahmen der nachstehenden Bedingungen Versicherungsschutz für Vermögensschäden aufgrund folgender Ereignisse (Cyber-Schäden):

- einer Netzwerksicherheitsverletzung;
- eines Bedien- und Programmierfehlers;
- einer Datenrechtsverletzung
- einer Cyber-Erpressung.

Eine **Netzwerksicherheitsverletzung** ist jeder unzulässige Zugriff auf das IT-System oder jede unzulässige Nutzung des IT-Systems eines Versicherten, insbesondere auch durch mitversicherte natürliche Personen.

Eine **Cyber-Erpressung** liegt vor, wenn einem Versicherten rechtswidrig

- mit einer Netzwerksicherheitsverletzung gemäß Ziffer I.1. oder
- mit einer Datenrechtsverletzung gemäß Ziffer I.3.
- gedroht wird und für die Nicht-Verwirklichung der Drohung ein Lösegeld verlangt wird.

Die Leistungen bei Versicherungsschutz

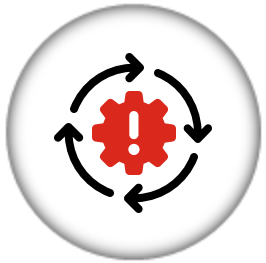
Soforthilfe im Notfall

- Experteneinschätzung zur Risikolage
- Empfehlung für Soforthilfemaßnahmen zur Schadenbegrenzung und Ursachenermittlung
- Ermittlung, ob eine Netzwerksicherheitsverletzung vorliegt

Cyber-Eigenschaden

z.B.

- Kosten für Krisenmanagement
- Kosten für IT Forensik
- Kosten für Rechtsberatung/PR Beratung
- Wiederherstellungskosten
- Lösegeld (sehr eingeschränkt)



Cyber-Haftpflicht

Schäden Dritter aufgrund versicherten Ereignisses

Cyber-Betriebsunterbechung

(optional)

#1 Schadenfall aus der Praxis (1/2):
Der Headhunter

Der Kunde:

– Ein mittelständischer Dienstleister (Personalberatung, Recruiting etc.) mit ca 60 Mitarbeitenden verarbeitet u.a. personenbezogene Daten. Typische Cloud-Tools sind im Einsatz. Backups sind vorhanden und gut gesichert (offline, separiert). Der Kunde fühlt sich gut aufgestellt und abgesichert.

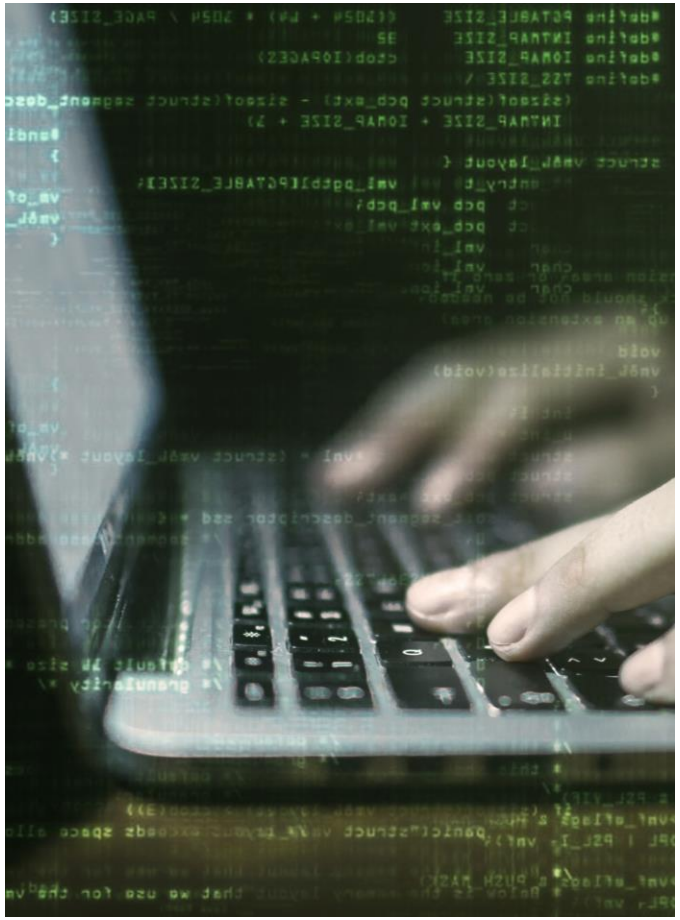
Der Vorfall:

– Unauffälliger Zugriff über kompromittierte Cloud-Zugangsdaten, keine Verschlüsselung, kein Systemausfall.

– Der Angriff bleibt wochenlang unentdeckt.

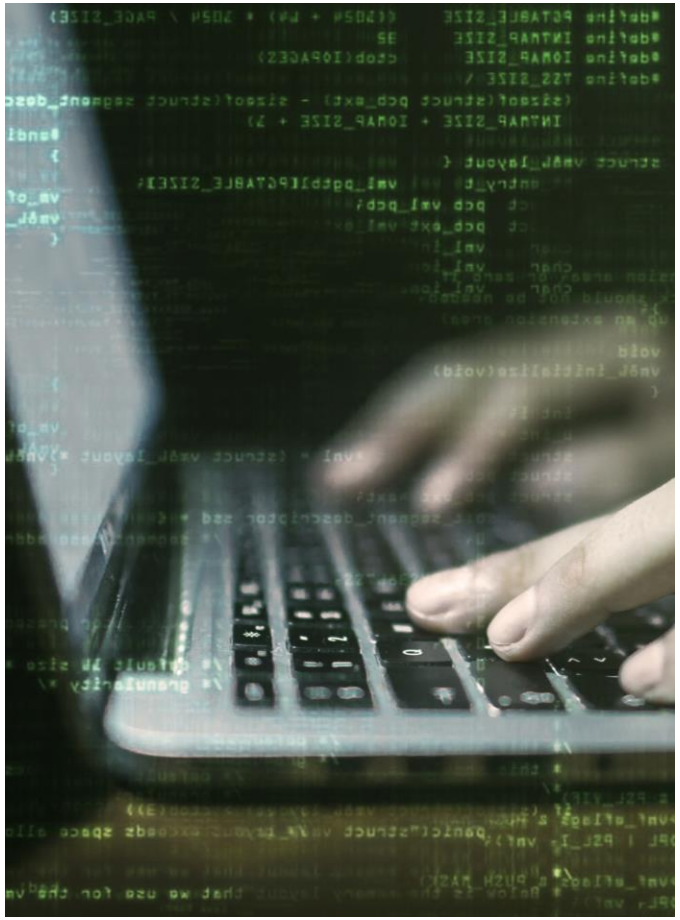
Die Eskalation:

– Email an die Geschäftsführung: “Wir haben vertrauliche Daten kopiert. Kundenlisten, Bewerberdaten, interne Verträge. Wenn Sie nicht zahlen veröffentlichen wir die Daten.”



#1 Schadenfall aus der Praxis (2/2):
Schaden

Drohende Datenveröffentlichung	IT-Forensik: Was wurde gestohlen/kopiert? Spuren der Angreifer?
DSGVO Pflichten	Kosten der Datenschutzberatung zu Meldung an Behörden und Betroffene Benachrichtigungskosten
Reputationsschaden	Kosten der PR-Beratung
Lösegeld	Betreuung bei der Abwicklung/ Verhandlung einer Lösegeldforderung Ausn.: Erstattung von Lösegeld
Strafrechtsschutz	Kosten im Zusammenhang mit Straf- oder Ordnungswidrigkeitenverfahren gg VN oder mitversicherte Person



#2 Schadenfall aus der Praxis (1/2): Supply Chain Incident

Der Kunde:

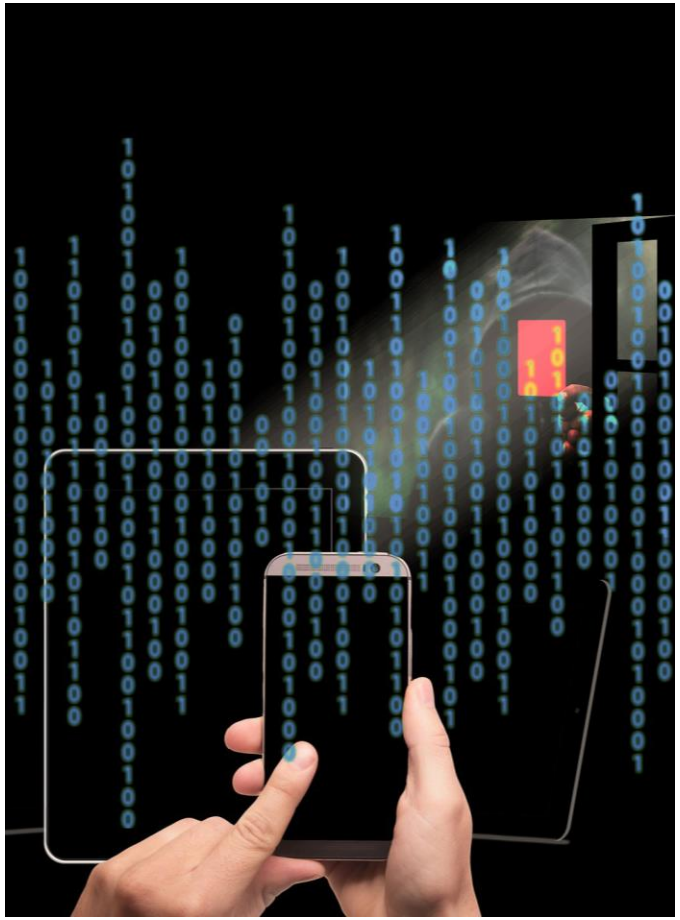
- Ein Managed Services Provider (MSP) übernimmt Remote Monitoring & Management. Er betreut mehrere hundert KMU-Kunden (IT-Betrieb, Patching, Admin-Zugänge).
- Dadurch besteht eine starke Konzentration (ein zentrales Tool/ ein Cloud Identitätsdienst), aber auch eine hohe Abhängigkeit (KMU haben oft keine eigenen Admin-Zugänge mehr)

Der Vorfall:

- Kompromittierung eines MSP-Admin Kontos. Der Angreifer nutzt legitime Fernzugriffe. Der Zugriff erfolgt dann auf Cloud Umgebungen der Kunden, Backups und Administrationsprotokolle.

Die Eskalation:

- Keine flächendeckende Verschlüsselung, sondern Drohung gestaffelter Datenveröffentlichung pro Kunde.



#2 Schadenfall aus der Praxis (2/2): Supply Chain Incident

Schaden-Besonderheiten:

Fokus klar auf Kommunikation und Zusammenarbeit

Herausforderung, die richtigen Dienstleister einzubinden und zu koordinieren:

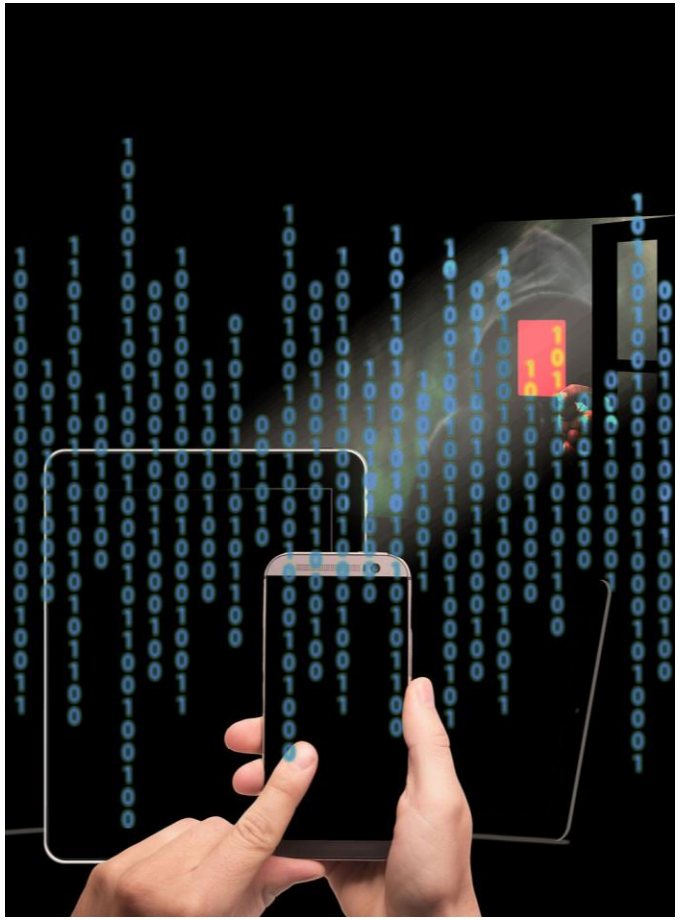
PR Berater

Forensiker

Datenschutzrechtsanwälte

VN und deren Mitarbeiter

Gemeinsame Entwicklung einer Strategie Hand-in-Hand.



Zusammenfassung: Ablauf eines Schadenfalles

1

Meldung über die Krisenhotline

- 24/7-Erreichbarkeit
- Schnelle Einbindung
- Erste Handlungsempfehlungen

2

Technische Soforthilfe durch den Krisendienstleister

- IT-Forensik & Analyse
- Unterstützung bei Meldungen
- Krisenkommunikation

Laufende Abstimmung & Prüfung durch Hiscox

- Prüfung Versicherungsschutz
- Gemeinsame Koordination
- Dokumentation & Bewertung

3

Deckungsentscheidung und zügige Regulierung

- Vertragsprüfung
- Erstattung versicherter Kosten
- Fallabschluss

4

Lessons learned / Best Practice

„Old but gold“

→ Awareness Schulungen, Phishing Tests

→ Sicherung der IT Systeme: Multi Faktor Authentifizierung, Segmentierung, Patchmanagement, Firewall, Offline Backup etc.

(Exkurs: CyberClear Plus 01/2026)

→ Im Schadenfall: Krisenhotline anrufen!

Cyber Readiness Report 2025

- Nur 4 von 10 KMU in Deutschland verfügen über eine adäquate Cyber-Versicherung
- Trotz gestiegener Investitionen und wachsender Sensibilität bleibt die Cyber-Resilienz vieler Unternehmen lückenhaft: Aktuell verfügen lediglich 40 Prozent der befragten Unternehmen über eine eigenständige Cyber-Versicherung. 38 Prozent gaben an, dass sie Cyber-Risiken im Rahmen einer anderen Police abgedeckt haben. Weitere 14 Prozent planen den Abschluss einer Cyber-Police. Damit sind aktuell sechs von zehn KMU in Deutschland nicht oder nicht ausreichend gegen Cyber-Gefahren abgesichert.

6 von 10 der deutschen KMUs sind nicht ausreichend Cyber-versichert

Quelle: Hiscox Cyber Readiness Report 2025 (www.hiscox.de/crr2025)

Cyber Maturity Check:

Wie widerstandsfähig gegen Cyber-Kriminelle ist das Unternehmen Ihres Kunden?

Wie gut ist das Unternehmen tatsächlich gegen Cyber-Gefahren aufgestellt?

Wenn Sie es genau wissen wollen, beantworten Sie die Fragen der internationalen IT-Experten und Unternehmens-Entscheider und sehen Sie, wie es genau um die Cyber-Sicherheit Ihres Kunden bestellt ist.

Legen Sie nach dem Klick auf folgenden Link los mit Ihrem eigenen Cyber Readiness Assessment!

HISCOX

Vielen Dank für Ihre Aufmerksamkeit